SECURITY OF COMPUTER SYSTEMS

One thing mankind has learned in the long course of human history is that whenever a new device or technique is introduced it is bound to have unforeseen repercussions, both good and bad. The computer is no exception. On the one hand, it has permitted us to perform logical and processing tasks undreamed of by those who built the first computers. On the other hand, it has given rise to a whole new field of crime in America. Nearly every month the newspapers and trade journals carry articles about ingenious crimes committed with the assistance of computer equipment. The business community is becoming increasingly concerned about protection against fraud and embezzlement in this area. The law enforcement community is only now coming to the realization that it has been woefully slow in recognizing this problem and is trying to catch up.

Similarly in the area of classified information, the computer has given rise to a whole new field of security problems. And, like the law enforcement community, the security community has been slow in addressing ADP security problems. The general feeling among security people has been that ADP security problems are technical and therefore had best be solved in coordination with technicians (computer people) who understand them. Most of our present security regulations were not written with ADP in mind and hence provide little or no guidance for security problems which are unique to the computer.

Perhaps the single greatest problem security people will be confronted with in the 1970's is that the changes in equipment and techniques employed

in information handling will come along in such a torrent that it will be a monumental task to cope with their security implications. The year 1970 marks the Silver Anniversary of the computer. Already it has permeated nearly all facets of our lives. Yet, those who are in charge of computer research and development tell us that technologically the computer industry is at a more strategic take-off position today than ever before. The security implications of this are awesome indeed.

One of the security issues which is receiving growing attention today concerns the use of resource-sharing (sometimes called "time-sharing)" computer systems for handling classified material. As you know, these are systems which consist of a central computer facility to which are linked a number of remote query terminals in the same building, in other buildings, or even in other cities.

The great advantage of such systems is that they provide a capability for simultaneous operation by many different users. In the central computer facility can be stored data bases of varying security classification. The remote terminals can be located in physical areas with varying levels of security clearance. In such a system, provision must be made to assure that classified information is released only to authorized individuals. Similarly, provision must also be made to assure that the information stored in the system can only be changed or deleted by authorized personnel.

Very briefly, the problem areas in resource-sharing computer systems fall into six major categories:

(1) Personnel. Computers, in themselves, have never committed a crime or been guilty of a security violation. It is only people who have

operated, or programmed, or maintained, or used computers who have committed crimes or caused security violations. This means that the security officer is faced with exactly the same personnel security problems found in any other field, and must pay special attention to the loyalty and experties of these categories of people in his organization.

The operator who is responsible for the minute-by-minute functioning of the system could deliberately or inadvertently cause a security violation by improper use of the system. He could, for example, replace the correct Supervisor program by an improper one. Since the Supervisor is analogous to a combined umpire and rule book at a baseball game, you can readily imagine what could happen if the operator should replace the Supervisor program. It cannot be stressed too much that the operator must understand what it takes to operate the system effectively and securely under any circumstances.

ILLEGIB

The programmer has ample opportunity to inject defects into the software either through error or by design.

The maintenance man could deliberately or accidentally rewire part of the equipment so that it appears to function normally, but, in fact, bypasses or alters the protection mechanism.

As far as the "user" is concerned, the central processor must make certain with whom it is conversing at all times. There must be some means built into the system for ensuring that only authorized personnel have access to the data bases through the remote terminals.

All of these personnel problems could be serious, but fortunately, they can be resolved by proper administrative and technical

procedures. In order to accomplish this, however, everyone involved in the system must be subject to a prescribed discipline and authority.

(2) Physical Security. Physical security is the first line of defense in any computer system. Without this, most other measures taken to protect classified information in a system are sharply degraded.

In a resource-sharing computer system, the area containing the central computer must be secured to a level commensurate with that of the highest security classification of the information in any of the data bases. Physical protection of the central computer room must be continuous because of the threat posed by the possibility of someone tampering with the equipment. Adequate controls must also be imposed upon all removable items in the computer room. By this I refer to such items as printouts, disk packs, punch cards, and magnetic tapes. As far as the remote terminals are concerned, they must be afforded physical protection commensurate with the sensitivity of the information which will or can be handled through them.

(3) Software. The variety and complexity of software employed in modern resource-sharing computer systems is so great that only a few basic principles can be addressed here. At the risk of gross oversimplification, the following general software principles should be observed in any secure resource-sharing computer system:

(a) Adequate security protection cannot be provided by software alone, no matter how complex and imaginative.

(b) The most critical portion of the software is the Supervisor (also called the Executive or the Monitor). The Supervisor

acts as the overall guard of the system. It is that portion of the software which internally manages job flow through the computer, allocates system resources to jobs, and controls information flowing to and from files and terminals. The malfunction or deliberate alteration of the Supervisor could couple information from one program to another; change the security classification of users, files or programs; or, at a minimum, clobber information in the system.

(c) One of the highest security risks in the operation of resource-sharing computer systems occurs where users at remote terminals are permitted extensive programming capability in many languages and with any compiler. In such cases, there is the risk that the user will thereby alter the Supervisor program and, almost literally, change the rules of the game.

(d) A file-query system which merely provides the user at a remote terminal the capability to access files using a set of fully checked programs is probably the least dangerous mode of operation in a resource-sharing computer system.

(4) Hardware. There is such a wide and growing variety of equipment and configurations used in resource-sharing computer systems that it is very difficult to generalize on desired security features. In brief, however, programs and data bases are stored in the main computer memory and in other storage devices such as tapes, disks and drums. A secure resource-sharing computer must be designed so as to prevent leaks between two or more programs or data bases which happen to reside in the computer simultaneously. It must also be designed so as to identify each terminal and its authorized user.

The principal hardware techniques employed for segregating programs and data bases are various forms of memory bounds protection devices. These must be sufficient so that any attempt to read or write outside the area of memory assigned to a given user will be detected and prevented. It should be stressed, however, that memory bounds protection can fail. Because of this, some believe that it is essential that a special program attempt to deliberately and frequently violate the memory bounds to verify that the bounds protection monitor is, in fact, working. This is particularly important after a cold start, initial program load, or maintenance.

In addition to memory bounds, the architecture of the computer must provide for privileged instructions. The set of privileged instructions must contain all input/output commands and also every command which could change a memory bound or protection barrier. Moreover, the design of the computer must be such as to ensure that only the Supervisor program can operate the privileged instructions. It is absolutely essential that the Supervisor program not be bypassed.

(5) Communications Links to Remote Terminals. Basically, the problem here is no different than that of sending classified information over any communications system. Adequate protection must be provided by means of any of the standard techniques (encryption, etc.) used in communications systems around the world.

(6) Administrative Procedures. Finally, the security of any resource-sharing computer system will rest, in no small part, on the

administrative procedures established for the system and the manner in which these procedures are enforced. There must be thorough indoctrination of all personnel involved in the system, particularly concerning actions to take in case of malfunction of the hardware or software. The system for identifying and authenticating users must be protected to the same extent as one protects the combinations to safes. There must be a carefully documented process of system certification before the system is permitted to handle classified data. There must be frequent testing of the system to ensure that it is functioning as designed. And, finally, I think the security people should make frequent attempts at penetrating and subverting the system in an effort to detect hidden flaws and vulnerabilities.

In the final analysis, the security of a resource-sharing computer system must come from an interlocking of (1) personnel security, (2) physical security, (3) hardware security, (4) software techniques, (5) communications security, and (6) administrative procedures. Exclusive dependence on one area (for example, software) must be avoided. We have now had sufficient experience with the day-to-day use of resource-sharing computer systems, and have subjected them to enough in-depth analysis, to have some confidence that we know the major problem areas with reference to security. If used properly and intelligently, and if subjected to frequent testing, resource-sharing computer systems employing today's hardware can provide acceptable protection to classified information. In fact, they can probably provide greater protection than many manual methods of handling information.

Looking toward the future, there is no doubt but that a wide variety of new equipment and techniques will be developed for the handling of information in the next decade. There will be a growing merger of computer and communications technology. This will be more of a chemical mixture than a mere matter of addition as each technology is changed in the process. Already we are beginning to see networks of computers which span our continent and extend into overseas areas. There will be a rapidly growing variety of remote access devices and computer-driven displays. We will see the introduction of new types of memories in computer equipment: magnetic thin film memories, plated wire memories, large-scale integrated solid-state memories, magnetic bubble memories, laser-driven optical memories, etc. There will be a wide proliferation of random access devices for the storage of very large files. Our concepts of file structure will become ever-more sophisticated.

By the end of the 1970's, it is likely that there will be a greater volume of classified material stored and exchanged in machine-readable form than in hard copy. This means that our concepts pertaining to the storage, retrieval, accountability, and dissemination of information will have to be changed and updated frequently.

The overall theme of this Seminar is "Security 1970 . . . A Departure from Tradition." If the security people of this nation are going to understand and solve the security problems which lie ahead in the fast-changing field of information processing, there will indeed have to be a number of significant departures from tradition. The education and training of

security officers will have to change drastically. Security policies and concepts will have to undergo frequent reappraisal. Administrative procedures for updating security manuals and instructions will have to be streamlined. New techniques for monitoring and testing the security of one's agency or company will have to be devised and continually updated. And, last but not least, extensive and imaginative research will have to be undertaken into the nature of security problems involved in information processing.

Perhaps the situation we are in can best be illustrated by an anecdote about a man who was riding on a train. As he rode along, he looked across the aisle and noticed that the man sitting there was an old professor of his. "Pardon me, sir," he said, "Aren't you Professor Shultz?" "Why, yes," replied the Professor. "You probably don't remember me," the man said, "but I had a class from you in economics 29 years ago." "Well, I'm delighted to see you again," said the Professor. "You were a tremendous Professor," the man went on, "I remember a great deal of what you taught us. I even remember the questions that were on the final examination." "Well, that is an odd coincidence," responded the Professor. "I just happen to have a copy of this year's final examination in my pocket. Would you care to look at it?" With that, he handed the questions across the aisle. The man read the questions and then, with a very puzzled look on his face, said, "Hey, Prof, these are the same questions you asked 29 years ago." "Yes, I know," said the Professor, "but the answers keep changing!"

The basic questions of how to protect classified information are the same as they always were. But, in the modern era of rapid technological developments, the answers certainly keep changing.

Next 1 Page(s) In Document Exempt